

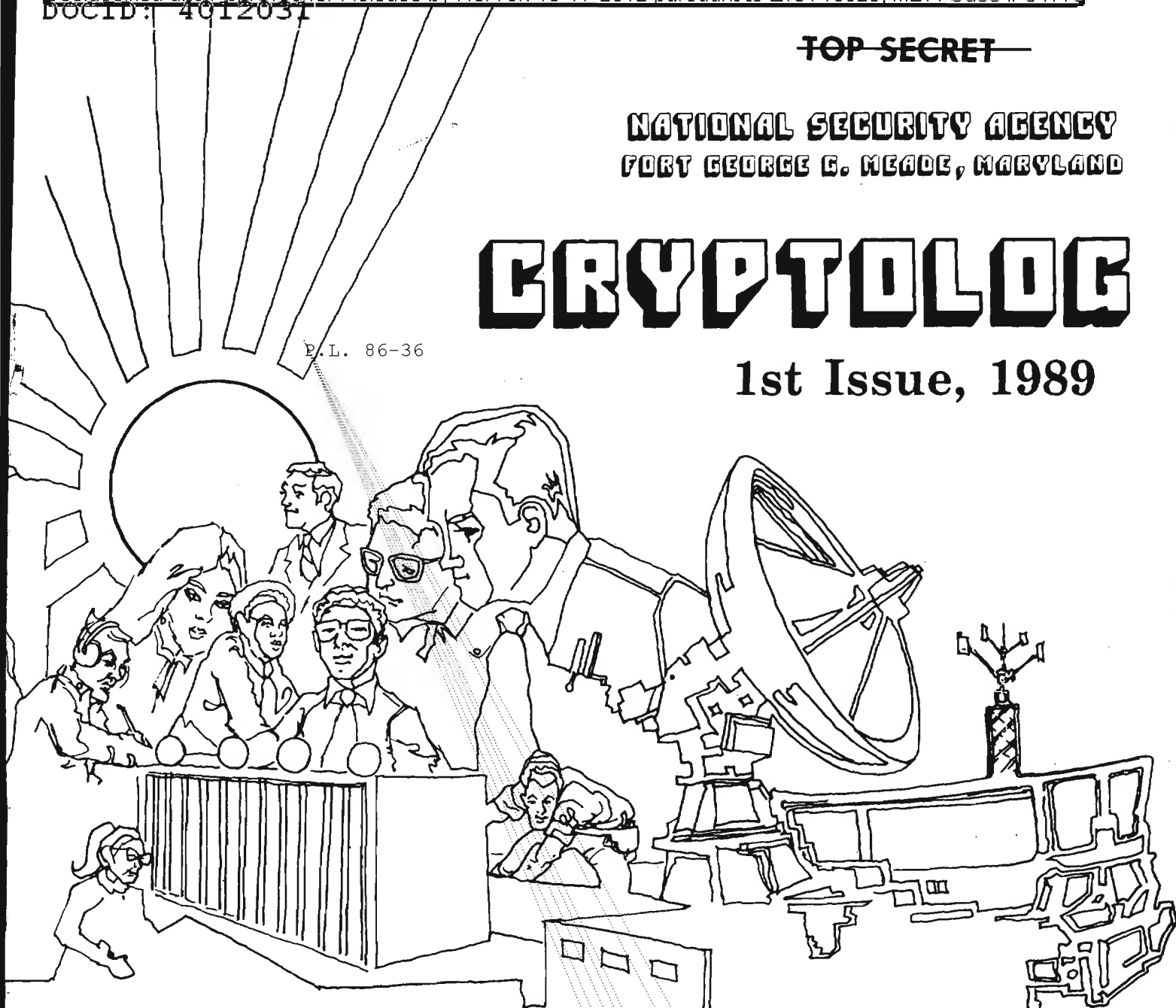
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

1st Issue, 1989

P.L. 86-36



WHERE ARE OUR TEXTBOOKS?	David Gaddy	1
QUOTE WITHOUT COMMENT		4
PROJECT TOTEMPOLE		5
GOLDEN OLDIE		8
DEFSMAC'S 25th ANNIVERSARY		9
BULLETIN BOARD		10
OUR NEIGHBORHOOD: ASQ 20	Vera Filby	11
FROM THE PAST		12
ONE CRYPTANALYST'S ONE-FOOT SHELF		13
CONFERENCE REPORTS: DARPA ON LANGUAGE MATHEMATICS	David Harris	15 19
REVIEW: BOOKS ON SIGINT HISTORY		21
LETTERS		24
CLASSIFICATION QUIZ		26
BONUS PUZZLE: MINICRYPTS #2	Bill Lutwiniak	27
NSA-CROSTIC No. 68		28
ON THE LIGHTER SIDE		29

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~

~~DECLASSIFY ON: Originating~~

~~Agency's Determination Required~~

~~NOT RELEASABLE TO CONTRACTORS~~

P.L. 86-36

CRYPTOLOG

Published by P1, Techniques and Standards

ABOUT YOUR SUBSCRIPTION

VOL. XVI, No. 1 1st Issue 1989

PUBLISHER

BOARD OF EDITORS

Editor (963-1103)

Computer Systems (963-1103)

Cryptanalysis (963-5238)

Cryptolinguistics (963-4740)

Index (963-4814)

Information Science (963-3456)

Information Security (972-2122)

Language (963-3057)

Mathematics (963-5566)

Puzzles (963-6430)

Science and Technology (963-4958)

Special Research Vera R. Filby (968-5043)

Traffic Analysis Robert J. Hanyok (963-4351)

Illustrators (963-6234)

..... (963-3738)

..... (963-6423)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, HQ 8A187

If you used a word processor, please include the
mag card, floppy or diskette along with your
hard copy, with a notation as to what equip-
ment, operating system, and software you used.

via PLATFORM mail, send to:
cryptlg@bar1c05
(bar-one-c-zero-five)
(note: no 'o')

Always include your full name, organization, and
secure phone; also building and room numbers.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1, HQS 8A187
Please do not phone.

Contents of CRYPTOLOG may not be reproduced or
disseminated outside the National Security Agency without
the permission of the Publisher. Inquiries regarding repro-
duction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the
authors. They do not represent the official views of the
National Security Agency/Central Security Service.

Maybe some day the Agency will have enough
money to buy equipment that labels periodicals
automatically and bundles them in zip code order,
just like commercial magazines. Until then, we'll
have to make do with a compromise, which in the
case of CRYPTOLOG, is subscriber lists. The
alternative is general distribution by organization.

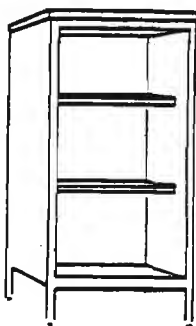
Perhaps a few words about CRYPTOLOG's distri-
bution are in order. The alphabetical subscriber
list is on an XT. Each record shows Date of
Information, Organization, Name of Subscriber.
There is also an Organization list showing Date of
Information, Organization, Building, Number of
Individual Copies, and Number of Organizational
Copies. When we're about to go to press, these two
lists are fed into a program which generates a list of
changes in distribution counts by organization for
Distribution (Y16) and a merged list that is sent to
a program on WINDMILL which generates a tape
for printing the subscriber lists that you -- or your
secretaries -- see. At this point the distribution is
cast in concrete for that issue. We mail the sheets
when it is time to proofread the Blue Line (the
photo proof before it goes to press). Note that we go
through this procedure for each issue.

Theoretically, CRYPTOLOG should hit the streets
a day or two after the subscriber lists reach you.
But things happen. The magazine may be bumped
by a higher priority at the Press. Or be held up in
Distribution -- they count off the copies and bundle
them by hand. So it may be ten days or so between
the time your office receives the lists and its copies
of CRYPTOLOG. Be patient. Wait. DO NOT CALL.

If you get too many copies, send us the spares --
maybe some other organization is short a few. If
you don't get enough copies, WRITE, do not call, for
more. And WRITE, do not phone, about a change of
address. We just can't cope with the volume of calls.

If anyone has better ideas about distributing
CRYPTOLOG, please send them on. We're always
looking for a better way.

~~FOR OFFICIAL USE ONLY~~



WHERE ARE OUR TEXTBOOKS?

David Gaddy, DSC

~~(FOUO)~~ According to legend at the National Cryptologic School, Minnie Kenny arrived on the scene as the new D/ADT a few years back and asked to see the library. There was no school library, she was told. Her response was, "Nonsense! Who ever heard of a school without a library?" Suiting action to words, she established the facility that was dedicated in 1982 and is still maintained by T51 (albeit now in constrained space, along with other crowded NCS activities at the moment). A visitor to the School today might well ask "where are your textbooks?" Would the answer be the same, "we have none"?

(U) Back in the summer of '65 our former colleague, sometime journalist, and classic jazz pianist [] deplored the lack of writing in an *NSA Technical Journal* article calling for the generation of professional literature. Ed's point, and a point with which most of us would agree upon reflection, is that professional literature is the outstanding characteristic of a profession. It is the means through which the profession is defined and through which the profession grows and evolves over time. It affords the opportunity to assert and to challenge, to advance ideas and to have them tested. It offers vitality; it encourages imagination and creativity; it exposes outdated thinking and procedures. It also does something else: In a 1988 memorandum to Agency seniors, enlisting their support in leading seminars, NCS Commandant Whitney Reed said, "lacking a more systematized institutional memory, we are heavily dependent on individual knowledge, recollections of lessons learned (or not learned), and acquired wisdom on the part of our seniors to guide the

education of the next generation of Agency leadership." More careful attention to professional literature would, in large measure, supply the need for "more systematized institutional memory."

~~(FOUO)~~ What do I mean by "professional literature" and by "textbooks"? I mean both in the broadest sense: articles, papers, monographs, manuals of a certain type--information in a form that can be studied, retrieved for reference, passed about. In the flowering that took place after Ed's 1965 article, the National Cryptologic School Press was announced by Commandant Frank Austin (the Agency's history program was under the NCS in those days) and the issuance of "Special Studies in Cryptology" began. *The Cryptologic Spectrum*, a somewhat more "popular," but classified, quarterly joined the highly respected and often erudite *NSA Technical Journal*. A variety of specialty-oriented house organs flourished among the groups, key components, and learned organizations, compensating in part for what I recall as a concurrent decline in case histories and system solution reports, once SOP but dropped because of resource reductions and larger workloads. But we were writing and we were reading. "Letters to the Editor" columns and articles offering a different viewpoint from that of an earlier one reflected the challenge and response, and a depth and quality of thinking was seen that was frequently lacking in daily memoranda. Such writing was the grist for textbooks.

(U) By "textbooks" I mean those things we could read and study as professionals and that would serve as the basis for teaching. When it

involves a record of past practice, this means history. But history can be relevant—indeed, it generally must be to be tolerated in a government agency. (It is not that "the old way" was necessarily the right way, but it was a way, and it might save time and effort for a later generation to be able to reflect on it.) It would add a sense of continuity, a kinship with the past. For example, I still have among my papers Bob Benjamin's 1964 revision of the 1955 *Fundamentals of Radio Traffic Analysis*, suitably worn and dog-eared, as befits a textbook and continuing reference. What is its late 1980s' counterpart? The syllabus of TA-103? Are we too busy doing, to reflect on the whys and wherefores? What is it we need as "textbooks"?

(U) We need service biographies of potential role models for a new generation, biographies to increase our appreciation of our profession, and our heritage from the military services and their civilian colleagues. We need studies of "lessons learned"—and not learned. We need accounts of actions and operations well planned and smoothly executed, and how—and those that weren't, and why. (Yes, I know, this is asking a lot of an organization or an individual. "Self-criticism," the Communists call it.)

(U) We need critical, reflective, analytical studies that will draw out the mind as well as informing—articles of a type so often encountered in Naval Institute Proceedings, perhaps the best military example of the professional literature I mean. We need imaginative, futuristic, "impractical" thinking. We need reprints of quarterly articles or technical papers, "convenience compilations," such as the Friedman lectures, the Boak lectures, *Collected Articles on Code*

Reconstruction, as compiled by Kate Swift and [redacted] We need "pop history," such as Ed Wiley's *On Watch*, produced by the NCS.

(U) What is our basic textbook today on C/A? On T/A? On reporting? On the concept of SIGINT support to a joint task force? On cryptology per se? Where are the writings for the apprentice, the journeyman, the advanced student?

(U) There is yet another consideration. With nearly a half-century or more behind us (depending on your choice of the starting date), we need doctrine—the distilled essence of our experience. We tend, rather, to have

procedural instructions. Studies—professional literature—would contribute to the development of doctrine. At the present time new students at the National War College receive a stack of 14 books (one of them an historical novel, by the way) to start their professional library. As a self-check, what would constitute yours? What 14 "must read" texts would you suggest to a newcomer in our ranks? What 14 or so do you believe every professional here should have read?

(U) From the vantage point of four years at the NCS, concerned with introducing the new generation (and outsiders) to cryptology, as well as life-long learning for the professional, I am excited over the potential I have seen in the new generation, but I regret all the more the disorderly shape of the heritage we offer them. Many of the oldsters have forgotten or have selective memories; many of the youngsters haven't discovered what was or felt the absence of what might be. Our sheer bigness removes the youngster from proximity to the oldster and the opportunity to eavesdrop (that is, learn from overhearing). As our profession has become more diverse and better known outside our fence, we've found unclassified writing about our once-concealed craft in books such as *The Codebreakers* and *The Puzzle Palace*, as well as journals, some good, some not so good.

(U) But who informs the professional or the neophyte which is which? It is all too human to reject what we personally know to be wrong, but tend to accept otherwise. We may accept and institutionalize untruths, such as the infamous Coventry bombing story. The continuing need for timely, informed book reports is obvious.

(U) Let me suggest some reasons for the state of things today: letting ourselves become too busy in other things; our incredible growth over the past decade; and, finally, not knowing what we're missing. We've been busy acquiring and defending. Our fascination with technology, and with "things" occupies so much of our time—another piece of equipment to master, another newer piece of software.

(U) We feel guilty taking the time to read and digest "unessential" classified matter in the office. We think about writing or rebutting, but don't take the time to do it. We see little evidence of reward for thoughtful exposition, of anyone caring. We often seem to be caught up

in careerism—ticket-punching—instead of honing the tools of our craft. Yet we bemoan the passing of the World War II generation and wring our hands about what industry calls "the assimilation of a new generation into our corporate culture," a culture we really have failed to define.

(U) There is probably another reason: The very computers that are enabling us to do easier word processing may be receiving the fruit of our individual creativity but denying it to others. Think-pieces probably reside in countless individual computer libraries. But professional literature must be generally accessible.

(U) For the most part, the professional literature I am describing must be classified. It must be generated, circulated, read, kept, and used at the office. It cannot be taken home for leisurely evening or weekend reading and contemplation, as with other professions. All the more reason, then, that it must be nurtured by a corporate concern. At the individual level that means allowing office time to read and reflect and write as part of our profession ... and not only permitting but encouraging subordinates to do the same. At the top it means having as Agency policy the advocacy and persistent defense of classified professional literature as essential to professional growth

The author, who chairs the NSA Cryptologic History Committee, solicits readers' views. Comments may be sent directly to him or to any other member of the Committee:

DDA	Robert L. Benson
DDI	Richard Proto
DDO	
DDT	
DDPP	
DDPR	
DDR	Thomas H. Cosgrove
ADIL	
ADT	Edward S. Wiley
GC	
J	

*Executive Secretary, Henry Schorreck,
T54, NSA Historian*

~~FOUO~~

and, indeed, survival when the paperwork reduction campaigns come upon us. It means recognition of, and reward for, contributions to the professional literature. (Although there is provision for it in our Personnel Summary, I wonder how often that section is considered at promotion or selection time.) It means providing conveniently located and equipped study facilities with access to classified professional literature.

~~(FOUO)~~ It may also mean a better corporate effort to institutionalize study and writing. The war colleges have had study groups of one form or another; CIA has its Center for the Study of Intelligence under their training establishment. The idea is an attractive one—the opportunity for a selected few to reflect, study, listen; to write; to teach; and then to cycle back into the fray, leaving behind a heritage of sorts and emerging with renewed energy and matured knowledge. And we do have a potential: As among T54, P1, the Director's Senior Council, the Director's Fellows, and other pockets here and there, we have mission responsibilities for study, reflection, and exposition, just as we do at the NCS, including its Cryptologic Education Fellows, where the product of such thinking is so needed for education and instruction in the form of case studies and textbooks.

~~(FOUO)~~ While great strides have been made over recent years in improving information support to analysts and analytical units, we are only beginning to apply the same attention to the automation of our records, a project well underway in T5. In time that will support not only historical research and writing but enable the study of topics that cut across target or major organizational lines. That is the very sort of research needed in developing doctrine, theory, philosophy—areas in which we are weak. Once we had the P1-sponsored Cryptologic Collection, the pride of Lambros Callimahos. There researchers could find assembled most of what they might want, whether classified or unclassified—technical reports, historical studies, news clippings, books. They could search for precedent in system usage beyond their target area or find copies of earlier studies on the subject of interest.

~~(FOUO)~~ Squeezed out of the Main Library because of a space crunch, the remnant of the Cryptologic Collection is consigned to T54 care in SAB 2, but is not being sustained. The

prospect of automating—and improving upon—that lost capability is a thrilling one.

~~(FOUO)~~ I must confess that, having spent six years across the street from T513, I had thought of "STINFO" as dedicated to the interests of Research & Engineering. Only recently did I learn of their indexing of internal publications. While it varies in coverage, STINFO would be my first place to check in seeking a bibliography of pertinent material on the subject of my research, and some day that index may be available online at my desk notwithstanding the horrible problem of access that must first be solved, given the caveats of the assorted documents received by T513.

~~(FOUO)~~ There are some hopeful signs that others are recognizing the need and addressing it within their spheres of interest. The IR Panel has found mutual benefit in assigning its interns to a tour in T54. Clubs and associations under the Council of Learned Organizations sponsor literary contests. Winners are recognized with publicity (sometimes cash) and publication.

(U) Publications such as *The Cryptologic Quarterly* and *Cryptolog* continue to manifest the qualities we need—one can only wish that they were monthlies, but the labor is much and the laborers few. Some serious studies are done in connection with courses at the NCS or elsewhere, but they may or may not see the light of day in general availability.

study of the personality types of Agency executives, done as a National War College project, later reached us in a modified, but concise and thought-provoking article in a publication concerned with the Productivity Campaign.)

(U) Perhaps, then, we are doing more to address the need, but are not adequately making the results known to the workforce. If so, the implications are the same: the professional literature I'm describing must, as I said, be generally available, and sufficiently current as to sustain reader interest. It must also be retrievable through subject matter, title, and author. That must be our goal. □

QUOTE WITHOUT COMMENT

.....
Extract from: "Reflections on the CA Essay Test" by Peter Jenks, *KEYWORD*, June 1971

The Question: 'Describe the attributes of a good working aid' was attempted by some 20 people. At least one respondent interpreted 'working aid' to be an assistant: e.g. a Crypt-Aide. A few described a 'good working aid' rather than its attributes. (Examiners survive these things and, it should be added, in a spirit of considerable generosity. Obviously responsiveness to the question is one of the things which must be assessed, but beyond that each essay is quite independently assessed in terms of its own premises.) Of the remainder, in any event, a surprising number of the respondents included an assertion much along these lines:

"When you are assigned to a new problem where nobody will tell you what the problem is, let alone how one goes about getting the answer, good working aids tell you what to do."

This was an unexpected answer. One's first instinct was to regard the point as marginal. Reinforcements from other essayists altered that; in the experience of far too many analysts it has proved to be of high importance. Granting this, one's second instinct was to accept the point as valid, giving credit accordingly, but to deplore the fact that it should be valid. What are our managers doing, or more to the point, failing to do?

The negative implication speaks for itself. Is it fair, though? Can it not be asserted that a manager, recognizing that a recurrent problem can best be dealt with by the use of well designed working aids which both conserve experience and preclude recurring reinvention, also recognizes that use of this aid is more edifying than hours of instruction? Can it not be asserted as well, that such an aid will not only enable the new analyst to go about his job on the most expeditious basis but, in addition that its very character will, to the inquiring mind, suggest the 'why' of that aid as well as the 'how'?

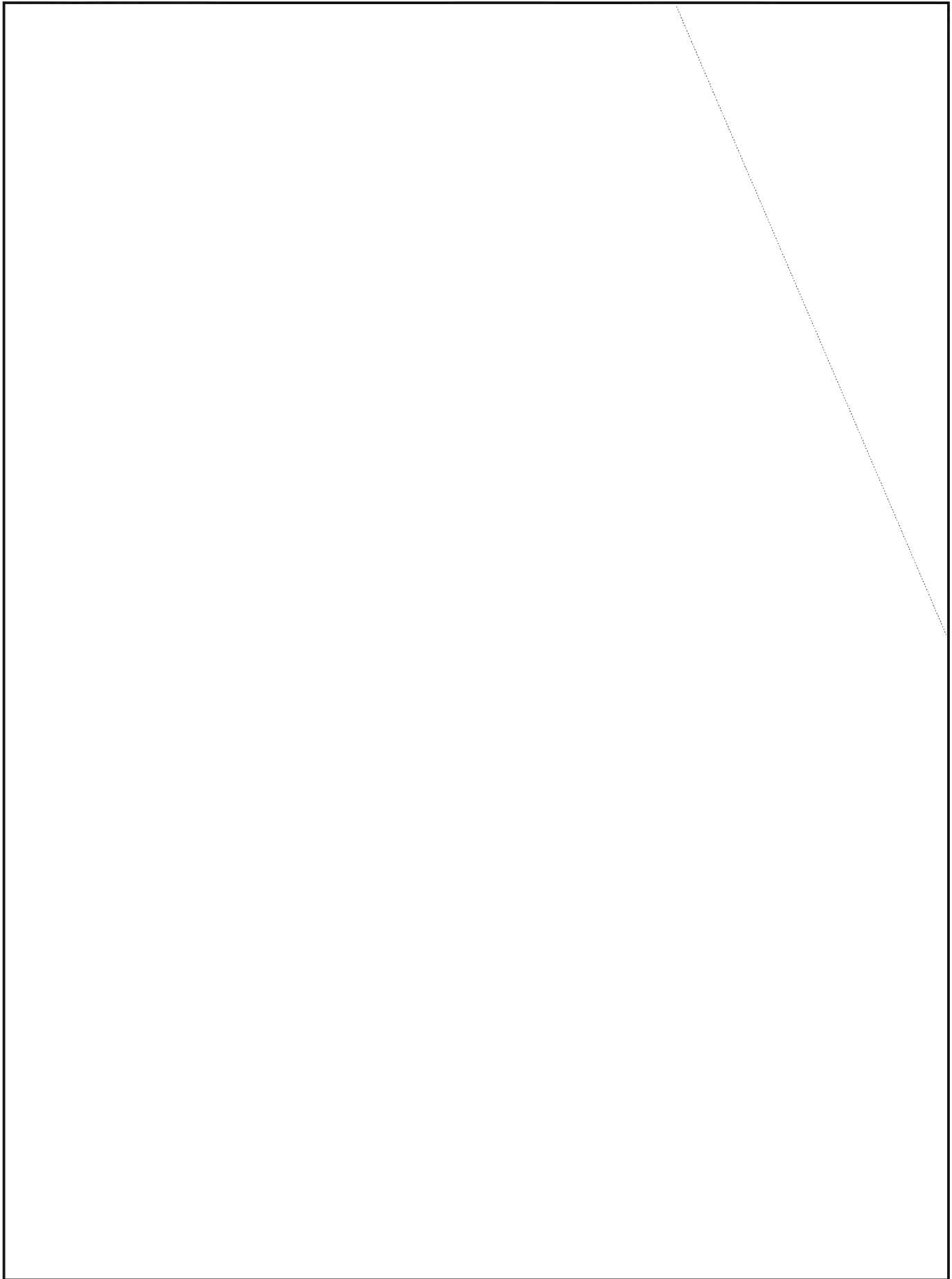
FOUO

Project TOTEMPOLE



1.4.(c)
L. 86-36

P.L. 86-36



~~SECRET~~



EO 1.4.(c)
P.L. 86-36

1st Issue 1989 * CRYPTOLOG * page 7

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~EO 1.4.(c)
P.L. 86-36*Golden Oldie*
CRYPTOPOEM

THERE WAS A LITTLE CIPHER
All digitized and stuff,
Who was tricky as the devil
But not secure enough.

She had no nice "top secret" beaux
To take on lengthy trips
She just went out with press reports
And other "routine" drips.

Her fellow codes and ciphers
Used to huddle in the safe;
And whisper unkind things about
This naive crypto-waif.

Whenever she was put to use
The others wreathed in smiles
Would snicker at her format and
Her quaint digraphic styles.

Then one fine day she got revenge
(The others all turned red)
For turning to her catty friends,
She snapped her nulls and said,

"Your cryptographic raiment
Serves to keep you well disguised,
But *I'm* the one who's had the fun
For *I've* been comprised - - "

Author unknown.

~~CONFIDENTIAL CCO~~~~SECRET~~~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

DEFSMAC'S SILVER ANNIVERSARY



P.L. 86-36

P.L. 86-36
EO 1.4.(c)

[redacted] Director, DEFSMAC, and

[redacted] Historian, DEFSMAC

(U) The Defense Special Missile and Astronautics Center (DEFSMAC) will celebrate 25 years of operations on May 3, 1989. DEFSMAC was established by direction of the Secretary of Defense in 1964 as a center to be staffed jointly by the Defense Intelligence Agency and the National Security Agency. The DIA contingent is a part of the Directorate for Collection Management (DC) while the NSA personnel are attached to the Deputy Director for Operations (DDO).

(S) The Department of Defense (DoD) charter for DEFSMAC specifies that it is to provide 24-hour surveillance of foreign missile and space activities, accomplish technical control of DoD intelligence collection systems directed against foreign missile and space events, provide technical support, including tip-off, to all DoD missile and space collection activities, and perform all-source current analysis and reporting on all detected foreign missile and space events based on initial site reporting. These responsibilities are carried out at a 24-hour operations center, with the support of a worldwide operational communications network, a dynamic, multi-discipline collection alerting and coordination effort, and analytic and technical data base resources.

[redacted]
(C) Among DEFSMAC's tasks is to provide earliest possible warning of preparations for foreign missile tests over the ocean to facilitate collection.

(C) The DoD community is increasingly looking to DEFSMAC for exercise participation, tip-off to new sensor systems, treaty support, timely provision of event-related information to operational commands, and collection coordination for strategic directed-energy weapon testing.

(S) The DoD's targets of interest in the foreign missile and space arena have grown dramatically in the past 25 years.

[redacted]
DoD and national level interest in the "Nth" country problem is demanding more time and resources as the potential grows for such countries to acquire ballistic missiles, chemical or nuclear weapons, and space capabilities.

(U) DEFSMAC occupies a unique location in the flow of initial site reporting. Its personnel perform very timely analysis of multisource

EO 1.4.(c)
P.L. 86-36

4th Issue 1988* CRYPTOLOG * page 9

P.L. 86-36
EO 1.4.(c)~~SECRET~~~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

data, and identify and report significant activity. These actions serve to bridge the gap between collector and user, to support prompt action by the scientific and technical intelligence community, and to meet the time-sensitive information needs of operational consumers.

(C) On 1 March 1989, after nearly two years of preparation, DEFSMAC began Space TACREP reporting to U.S. Space Command and others in support of Department of Defense Space Policy initiatives. This is the first step of the implementation of time-sensitive support to military commanders under a new function called Operational Foreign Instrumentation Signals Intelligence (OPFIS). Without this service, operational military commanders would not have access to time-sensitive information on the status of foreign missile and space weapon systems and to potentially significant improvements, or even, to entirely new systems that might be otherwise overlooked or whose analysis might be significantly delayed.

(U) On the occasion of its 25 Anniversary, the men and women of DEFSMAC would like to take this opportunity to salute the DoD, the Intelligence Community and Executive Agency, organizations we serve, and particularly our parent agencies, DIA and NSA. DEFSMAC's next 25 years promise to be even busier than its first 25. We look forward to continuing and improving the services and productive relationships. □

BULLETIN BOARD

FOR RUSSIAN LINGUISTS

(U) The complete Russian Handbook of Spoken usage is in press. It includes the first three volumes which were published individually (the letters A through Φ) as well as a new section covering the letters X through Я.

(U) The Handbook is an unclassified reference containing detailed information about the spoken Russian language. Entries are arranged alphabetically by the principal word in the phrase. It includes:

- ▶ constructions characteristic of the spoken language
- ▶ regional, uneducated, and other non-standard words and forms
- ▶ points of syntax and usage
- ▶ particles and combinations of particles

~~(FOUO)~~ Individuals in A2, A4, A6, E3, and the field should order copies through their organizations. Others may order copies **BY MAIL** directly from the author: P16, HQS. Telephone orders will not be accepted.

P.L. 86-36

LIBRARY OF UTILITY SUBROUTINES

~~(FOUO)~~ G964 has developed a library of utility subroutines to be used with the common data format discussed in CRYSCOM Recommendation #5, October 1988. The library has been successfully ported to SUN, JEPX, CONVEX, and IBM/AT computers. The source code has been written to allow conditional compiles so that a small, medium, or large version of the functions can be created on the AT.

(U) The library is modular so that programmers need select only those routines that are needed, thus keeping the program code to a minimum.

~~(FOUO)~~ Address your inquiries and suggestions to 963-5317.

P.L. 86-36

~~SECRET~~~~HANDLE VIA COMINT CHANNELS ONLY~~

Our Neighborhood: Airport Square 20



Vera Filby, E4

One bright December day a group of us from the Intelligence and Analysis Department of the National Cryptologic School rode over to Airport Square 20 to inspect our new quarters. We were to occupy the entire top floor of the latest Airport Square building and were to be the only occupants for an indefinite period of time.

We found a four-story brick and glass building graced by a fringe of trees that had somehow been allowed to survive from the woods that until recently covered the land hereabouts. Entering the lobby, we glimpsed the expanse of a softly lit atrium beyond the security desk. We took a rather childish pleasure in our ride up the glass elevator with its frame of sparkling lights. We emerged in the corridor alongside the atrium, and from there we looked down across a scene of hanging plants and banners.

The future office and classroom spaces, still bare of most of the furniture, were bright with light from the jalousied floor-to-ceiling windows on all sides. As we looked for our allotted spaces we paused to admire the scenery on the way, most especially the broad prospect from the north side and a clear view right down into the Inner Harbor. That was a surprise.

We moved in over the Christmas holidays, and early in January the first students started to arrive. They seem to like it here too. For one thing, since the building is only one quarter occupied, parking is no problem. Some of them like to sit on the floor outside the atrium near the windows and enjoy the view while eating their lunch. The other day a couple of students were speculating on how many more Airport Squares there would be.

The answer to that question is not yet certain, but Mr. Gregory E. Masi of Dickinson-Heffner Incorporated, the developer, was glad to tell me

when I asked him that during the next 7 to 8 years, 10 or 12 more buildings will be constructed, filling in the gaps in the 124-acre Airport Square campus and continuing the development of Airport Square Technology Park, located to the north and east. The name Airport Square Technology Park is now applied to the entire 300-acre project, which when completed will have created 3.5 million square feet of office space. Airport Square Technology Park is a totally integrated project, with the developer performing every part of it - land acquisition, development, design, construction, landscaping, gardening, marketing, financing, leasing, management, and maintenance.

Dickinson-Heffner's ventures in this area began in the mid-1960s with the building we knew as FANX-I when it was used for NSA operations. FANX-II was built as a warehouse. FANX-III was designed to NSA specifications, supplying 450,000 square feet of office space. Some years later Airport Square 1 appeared, and since then about a dozen three- and four-story Airport Squares have been built and occupied by a variety of tenants.

"Why does Airport Square 20 have four stories?" I asked Mr. Masi. "Why not two? Or five? Why not a highrise?"

"The answer to that is easy," he said. "We track the real estate market closely, and this is what people want - what they need." What they need translates to a first-class modern suburban commercial building which can provide a high quality workplace environment inside and outside. If it happens to have a greenhouse atrium, so much the better. When a building is constructed for the speculative market, it may have to be altered for the new tenant.

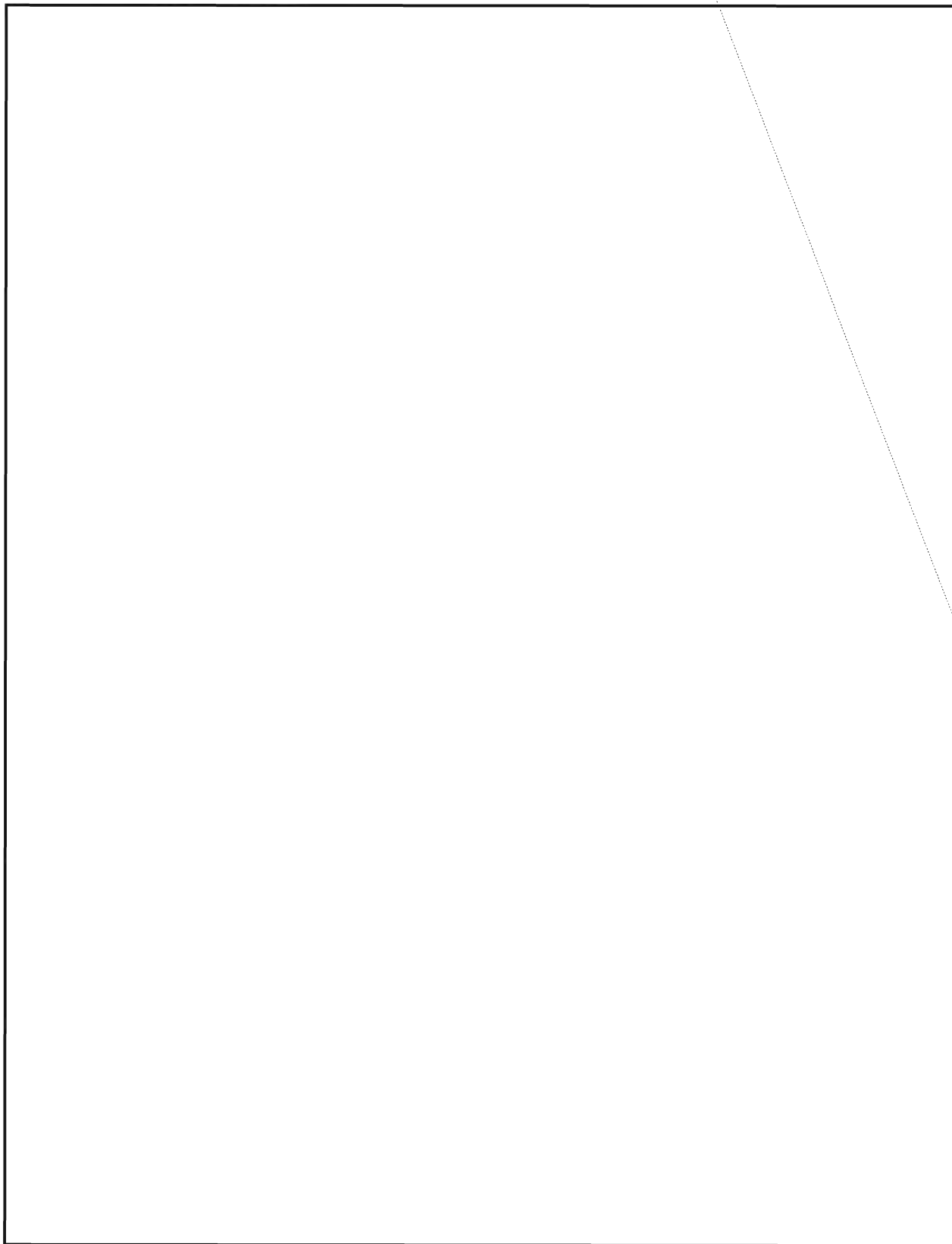
This happened with Airport Square 20. Before we could move in the floors had to be raised 9 inches to accommodate the wiring for our computers and especially for networking our long-awaited new computers. They were acquired to give us the means to develop computer assisted and computer based training and new applications for the continuing modernization and enhancement of our courses.

We are now wired up, settled in, and in business - and getting ready for new initiatives in the use of computers in training and education. □

~~TOP SECRET UMBRA~~

FROM THE PAST

EO 1.4.(c)
P.L. 86-36



~~TOP SECRET UMBRA~~

~~CONFIDENTIAL~~

ONE CRYPTANALYST'S ONE-FOOT SHELF

Reprinted from *KEYWORD*, January 1972



P.L. 86-36

P16

~~This article is classified C-CCO in its entirety~~

Can the cryptpie build a personal technical library which is adequate for his needs, but small enough for ready reference without resort to indexing, and compact enough to fit in his desk? This is in essence what CA interns ask after a first encounter with the CA library. My answer to them is that it can be done, and I hereby offer some suggestions as a starting-point.

Technical references can be sorted roughly into three types: 1) the general works that one might want no matter what the assignment; 2) special working aids that pertain only to a certain target or type of system; and 3) guidelines or aids traditionally distributed to entities such as section or branch rather than to individuals, usually because they are scarce or because they require frequent updating.

We will consider just the first category, the basic books for the permanent library that will have to be dragged around with every move. It is understood that the cryptpie has, for the duration of a particular assignment, the working aids that are purely local, such as Microbian word-pattern lists and Elysian pro-sigs. (He has a responsibility to see that working aids that he no longer needs are turned in or otherwise given a good home; the CA library, not the burn bag, is the proper repository, should the problem be dropped.) Machine ciphers, teleciphers and codes are not included in the basic books, not only for reasons of space, but also because the former two are usually worked in special sections and bookbreaking is seldom entrusted to the "pure" cryptpie.

The publications below total almost a foot, and that's just about the amount of space left over

in a desk file drawer when it's used to file legal-size folders; hence, the Basic Foot.

Remember, these are the suggestions of one cryptpie. Others might make other choices out of the works now available, and new publications come out from time to time which must also be considered. Watch for the Cryptanalyst's Statistical Handbook, soon to be issued by P1, and Virginia Jenkins' textbook Practical Diagnosis, now in working draft form. That one foot of drawer space will hold an amazing amount of cryptologic knowledge, if carefully managed.

MILITARY CRYPTANALYTICS, PART I AND PART II by L. D. Callimahos and W.F. Friedman

Everyone knows of MC I & II, and to many a non-cryptpie they are the Alpha and Omega of cryptographic literature because for years that's all that was generally available. Actually, together the volumes represent the Alpha; the Omega will be reached in that infinity where parallel lines meet.

MC I & II are the cryptpie's bible, wherein are expounded the precepts of "the science of cryptanalytics and the art of cryptanalysis"; it is here that the foundations are laid for the solution of any cryptographic system. The two volumes also comprise a handy refresher for working long-forgotten systems. The junior analyst fresh from class, I know, will find it hard to believe that next year he will not remember the niceties of solution that are so vivid in his mind now.

STANDARD REAGENTS AND DIAGNOSTICIAN'S DICTIONARY by I. J. Good (Blue Ribbon Series, Monograph No. 11)

This exceptionally well-written paper is considered by many cryptpies as the best friend to take along when you lay siege to a difficult system; it will advise, comfort and sustain you, and keep you from straying. It contains specifics in compact form on how to go about things, including thinking, and so it is a practical handbook as well as good reading that invites dipping into. And the cryptpie who seeks guidance in these pages when the prospects are gloomy will come away enlightened, and heartened and refreshed by the uplifting and optimistic tone.

~~CONFIDENTIAL~~~~HANDLE VIA COMINT CHANNELS ONLY~~

~~CONFIDENTIAL~~

This most valuable tome, unfortunately, is out of print, and no reissue is planned for the near future. If you do not have a copy, make friends with someone who does, especially if he is about to retire. Meanwhile, there's a copy in the CA library that you can read.

BASIC CRYPTOLOGIC GLOSSARY (a new edition is just out)

COMBINED GLOSSARY OF TRAFFIC ANALYTIC TERMINOLOGY

COMMUNICATIONS IDENTIFICATION GUIDE: Volume III, Operating Signals

The reasons for having the first two are obvious; the third book lists the Q and Z signals and their meanings. The three volumes fit nicely in a looseleaf binder.

ARS CONJECTANDI: THE FUNDAMENTALS OF CRYPTODIAGNOSIS by L. D. Callimahos (Blue Ribbon Series, Monograph No. 18)

It's neatly put in the foreword by Dr. Tordella: "This monograph represents a milestone in cryptologic literature: it is the first detailed and comprehensive exposition of the fundamentals of cryptodiagnosis, treating the techniques and procedures of manipulating data and recognizing and interpreting phenomena. Broadly theoretical in its treatment of the principles of diagnosis, it is applicable to both manual and machine cryptosystems, whether the diagnostic examination is performed by manual methods or with machine aids.

"Any cryptanalyst, whether he has two years; or 20 years' background, will profit from the study of this pioneering work. For the experienced cryptanalyst, it is an indispensable *vade mecum*."

THE CRYPTANALYSIS OF CIPHER TEXT AND PLAINTEXT AUTOKEY SYSTEMS by L. D. Callimahos (Blue Ribbon Series, Monograph No. 19)

This monograph is an advance publication of two chapters of MC III, which is still in preparation. If you're working on unknown systems you need this, even though autokey isn't very common. Maybe it isn't common because it hasn't been found!

Watch for other parts of MC III as they come out in the Blue Ribbon Series.

COLLECTED PAPERS ON CRYPTANALYTIC DIAGNOSIS (S-194,074)

These interested papers range from the philosophical through the theoretical to the practical. Some are reprints and others are newly presented; all bear re-reading. Mr. [redacted] artical may shock some by its very title: "Is the Index of Coincidence Obsolete?" but it will prompt thinking about statistical tests in general. It should be mentioned that [redacted] appears to be the missing link between the mathematicians and the cryptanalysts, for his exposition is understandable to a crippe who came in through the liberal arts.

P.L. 86-36

THE SOLUTION OF TRANSPOSED CODE AND DOUBLE TRANSPOSITION SYSTEMS by H. D. Siegel (Blue Ribbon Series, Monograph No. 1)

In the foreword Mr. Rowlett said, "This paper by Helen Siegel, issued originally in 1948, is the first to be published [in the Blue Ribbon Series] because of its established reputation as an authoritative reference in dealing with transposition systems." It still is the authoritative reference.

RYE GUPPY MANUAL FOR CRYPTANALYSTS

The GUPPY programs give every crippe the equivalent of 100 top-flight, speedy, accurate and indefatigable crypt aides 'round the clock. The manual also serves as a resident consultant—just by reading through the descriptions of programs a crippe may find another was to study phenomena or even another approach to the problem.

LOOSE LEAF BINDER, Ad Lib.

This is probably the most valuable item in your collection, for it contains your own selection of handy-dandies. [redacted]

Whatever the contents, its dog-eared appearance proclaims it as your nearest and dearest. This is what you save in a fire!

P.L. 86-36

~~CONFIDENTIAL~~~~HANDLE VIA COMINT CHANNELS ONLY~~

Conference Report



P.L. 86-36

DARPA Speech and Natural Language Workshop
February 21-23, 1989, Philadelphia, PA

P16 to obtain copies of related papers and for further information.

Reported by: P16

OVERVIEW OF SPEECH RECOGNITION

Several Agency personnel attended the Spring DARPA Speech and Natural Language Workshop which presented ongoing research results and projections for DARPA-funded programs. The current budget for this research area is \$11M and will be cut by 15% for the coming year. In FY90 speech research will account for 75% of total budget of the Speech and Natural Language Division, while the remaining 25% will be applied to Natural Language research programs. Some attendees explained this discrepancy in terms of the new role of natural language research in speech processing.

A new program, entitled WHISPER, will provide an additional \$10M over the next three years. WHISPER is jointly funded by NSA and Rome Air Defense Center (RADC).

J. Makhoul: BBN Laboratories Incorporated

Areas of speech recognition are focused on the transcription of speech into words. Speech Understanding (SU) includes actions based upon the speech such as data base transactions and message gisting, and require natural language processing capabilities. This is an area of research that needs more emphasis. Without Natural Language Understanding (NLU), Spoken Language Systems (SLS) are limited. Computer architectures and software are necessary for real-time speech processing functions. More research is required on the topic of spoken language acquisition and modeling. Training opportunities in speech and language processing for undergraduate students should be expanded. There is much attention to Air Traffic Control (ATC) as a model for defense applications.

OVERVIEW OF NATURAL LANGUAGE

M. Marcus

Past research focus has included augmented transition networks, natural language interface (NLI) to database systems, and expanded context-free parsing. There is a DoD thrust on replacing query languages with NLI. Current areas of research are focusing on unification grammars, lexical functional Grammars, computational semantics and discourse analysis. Much research is depending on a wide range of *a priori* knowledge about the world or operational domain. New research should focus

The following notes summarize conference activities. Interested individuals can contact

P.L. 86-36

on prosody for SLS, machine translation (MT), stochastic and symbolic techniques for learning grammar. The Japanese have a major effort in MT that will produce a wave of commercial natural language products soon. DARPA does not have an MT program.

TUTORIAL on NATURAL LANGUAGE

Grishman, New York University

Natural language technology is used to produce man-machine interfaces (MMI) and for automated message processing. There are two distinct views, computational and theoretical. Two major goals are syntactic analysis and semantic analysis. The former is more feasible.

Semantic analysis requires an experiential base of real world knowledge in order to be effective.

TUTORIAL on SPEECH

E. Neuberg, IDA, Princeton

Neuberg presented an overview of articulatory phonetics, acoustic phonetics, and phonology. He then provided a technical introduction to speech recognition.

INVITED TALK ON PROSODY

Pierrehumbert

Pierrehumbert delivered the invited talk on prosody. She demonstrated that prosodic features convey semantic and pragmatic information. She also showed that phonological phrasing does not always match syntactic groupings. In light of the role that prosody plays in understanding spoken language, Pierrehumbert suggested that speech recognition systems be built in narrow domains so that these systems can attempt to incorporate the systematic use of prosody.

PERFORMANCE EVALUATION

*Natural Language Evaluation Workshop:
Palmer, Unisys*

Two methods of evaluating natural language processing (NLP) systems were presented. The black box method analyzes user viewable input/output, modularity and the man-machine interface. The glass box evaluation method considers a systems underlying theory, efficiency, and extensibility. The meeting was

successful for testing syntactic systems but no agreement on semantic testing could be reached.

DATABASES

Text Collection: Marcus, U. of Pennsylvania

There is an emphasis on collecting test corpora of text. There are many different sources offering free but licensed text corpora for use in the research community.

Spoken Language: Doddington, Texas Instrument

Efforts to assemble a data bases of spoken language examples will receive 1.5M dollars over five years. There is a new effort to collect spontaneous speech examples in different scenarios.

INTEGRATION OF SPEECH AND NATURAL LANGUAGE

BBN: Stallard, Roukos

Because understanding spoken language requires actual understanding of language, BBN is Integrating its natural language component with MIT's speech recognition system. Basically, itsr system takes a word lattice as the output of a speech recognition system and then uses its natural language component (syntactic, semantic and pragmatic components) to identify the input sentence.

Stanford Resarch Insitutute International: Moore

SRI is attempting to integrate the architectures for speech recognition (SR) and natural language processing (NLP). Because of problems with word lattices and a serial connection between SR and NLP components, SRI is using a dynamic grammar network. In this system, a natural language parser incrementatly generates a grammar state transition table used in the Hidden Markov Model (HMM) speech recognition architecture.

University of Pennsylvania: Steedman

The University of Pennsylvania is investigating the integration of syntax and entonation in a combinatory grammar because of the inadequcy of present theories of syntax for processing speech. They propose using a combinatory categorial grammar which provides the notion of a syntactic constituent that is the same as

the notion of a sense-unit in a recent theory of intonation.

Carnegie Mellon University: Ward

CMU is just beginning to research recognition of spontaneous speech. Because of limitations of current recognizers, they will use a HMM work recognizer and create a phrase lattice. Syntactic constraints will operate locally and semantic globally. This is a system which will use a tighter grammar at the recognition level and produce a phrase output.

MIT: Seneff

MIT is developing TINA, a natural language system for speech understanding tasks. The system integrates ideas from Augmented Transition Networks and Lexical Functional Grammars. Probability assignments on arcs provide the basis for a best-search parsing strategy.

Texas Instruments: Hemphill: Picone

MIT is researching the integration of natural language models with statistical probabilities in speech understanding. They are using a chart parser with stochastic regular grammar in combination with rule and observation probabilities.

Carnegie Mellon University: Young

CMU is using a higher level sources and constraints to predict content and thereby reduce complexity in speech recognition. These sources include the dialog model, task semantics, general world knowledge and user knowledge.

NATURAL LANGUAGE RESEARCH

New York University: Grishman

NYU discussed its telegraphic speech handling system, PROTEUS. Basically, a general English grammar is relaxed, allowing the omission of subject and preposition. To control relaxation, the system applies local semantic parsing and imposes a penalty for each omission.

University of Pennsylvania: Joshi, Webber

Joshi is studying the equivalences of grammars and lexicalized tree adjoining grammars. In a tree adjoining grammar, each lexical item has

its own tree. Once the trees are identified, the trees are adjoined. Webber is researching cooperative response generation and discourse phenomena, particularly clausal reference.

Unisys: Palmer

PUNDIT is Unisys' natural language understanding domain specific system. Presently, the system handles about half of the input data composed of casualty report and rainform messages. Developers are extending the linguistic coverage and building tools for development. They are also working on interaction among the syntactic, semantic, and pragmatic components and are creating a more sophisticated interaction with knowledge bases.

SRI: Hobbs

TACITUS is a message understanding system which extracts information for database updating. Basically the abductive inference scheme in the system produces a logical form of a sentence in the message and then tries to prove it. For this system, interpretation of a text equals the minimal explanation of why the text would be true.

BBN: Bobrow

A major problem in applying natural language systems to different applications is the cost. To reduce the cost involves a) reducing the amount and complexity of application-specific knowledge, b) matching the interface to user capability and information needs, and c) reducing marginal costs. To reduce the cost of porting their natural language interface to a new database, BBN developed Knowledge Acquisition (KNACQ).

IBM: Byrd

IBM is developing a system to disambiguate dictionary entries. The system would hold word senses in a hierarchy and some information necessary from the context for disambiguation. This would be a lexical knowledge base, not a world knowledge base.

BBN: Crowther

Crowther is building a database from on-line reference works, like dictionaries and encyclopedias. He is researching the procedures

for building databases and retrieving information from databases.

Information Sciences Institute, UC: Kasper

ISI is developing a more efficient means to link applications (expert systems) to PENMAN, their text generation system. A subordination tool to coordinate knowledge in Penman and a Sentence Planning Language (SPL) are now provided.

UC at Berkeley: Wilensky

Wilensky is developing a natural language interface to help UNIX users, called UNIX Consultant. Presently, Wilensky is working on knowledge acquisition for the project.

New Mexico State: Hartley

Researchers have made three proposals to DARPA, two AI projects (model generation reasoning and resolution of conflicts in belief systems) and a project to evaluate parsers.

PERFORMANCE TASK PROGRESS

CMU: Rudnický

CMU researchers are developing a speech recognizer (SPHINX) and an interface for a spreadsheet task.

Dragon Systems: Baker

Dragon Systems is developing a system for interactive transcription for any subject. The system will have an open vocabulary and interactive error correction.

Unisys: Dahl

Unisys is developing a spoken language interface to an expert system (KSTAMP) for system maintenance.

MIT: Glass

MIT is developing a system called Knowledge Navigator. The system will allow the user to locate objects within an area and give directions to locations within the area.

BBN

BBN is developing a spoken language system to make database queries. The system will be developed from an existing database and a real-

time speech recognizer. The task domain is personnel records.

SRI: Price

SRI is developing a spoken language system for travel planning.

TECHNOLOGY TRANSFER

BBN: Bates

BBN ported PARLANCE (a natural language interface to SQL) to a Navy database by using a porting tool called LEARNER. LEARNER creates the domain-dependent knowledge bases that PARLANCE needs.

Dragon Systems: Baker

Dragon System discussed a number of different applications, some of which were successfully transferred to the commercial applications for which they were originally designed.

IBM: Davis

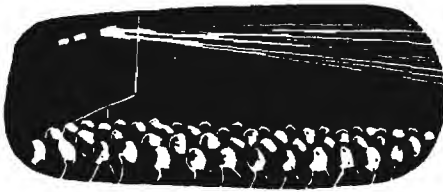
IBM has developed a real-time 20,000-word speech recognition system called TANGORA. In this study, IBM attempted to identify performance factors in order to develop behavioral strategies to improve the users' interaction with the system which requires some user speech modification.

ANSWERS TO

CLASSIFICATION QUIZ, p. 26

- | | | |
|-----|---|-------|
| 1. | e | |
| 2. | d | |
| 3. | d | |
| 4. | a | |
| 5. | c | |
| 6. | e | |
| 7. | a | |
| 8. | d | |
| 9. | c | |
| 10. | b | |
| 11. | a | and e |
| 12. | b | |
| 13. | c | |

~~CONFIDENTIAL~~



The Fourth SIAM Conference on Discrete Mathematics, San Francisco, June 1988

Reported by: David Harris, R51

~~(FOUO)~~ This was an outstanding conference on discrete mathematics, with many talks of interest to the Agency. We should continue to attend such conferences in order to gather the fruit being made available so cheaply. We should also look into some of the consequences. I suspect there has been some effect from Agency participation in conferences, in the direction of convincing academics and mathematicians from industry to see us as human. We also had the usual variety of informal discussions with outside academics.

(U) Technical highlights included:

- (U) A talk by Carl Pomerance on the use of number theory in cryptology.
- (U) A session on applications of number theory, with talks by Odlyzko (Riemann Hypothesis), Lagarias (multidimensional continued fractions), and Sarnak (Ramanujan graphs).
- ~~(C)~~ A session of invited talks on cryptology, including talks by McCurley (discrete logarithms), Goldreich (zero knowledge), and Crepeau (secret sharing). The McCurley talk was particularly alarming, in that it stressed practical wisdom.
- (U) A somewhat disappointing session of contributed talks on cryptology, including talks by McCurley (Buchmann-Williams cryptosystem), Bailey (Ferguson's algorithm for multidimensional continued fractions), Elia (application of linear error correcting codes to communications security), and Shoup (factoring polynomials over finite fields with a minimum of randomness).
- ~~(C)~~ A session on the use of Cayley graphs in communications networks, including talks by Cooperman, Fellows, Krishnamurthy, Blaha, and Faber. [redacted]

A talk by North on the use of graphics to simplify lattice structure.

- (U) A session of invited talks on irregularity and discrepancy, featuring talks by Spencer, Voigt, and Niederreiter. Possible applications include looking for non-randomness in apparently random data, designing super-flat sequences (especially for use in numerical analysis), and tests of randomness in general.

- ~~(C)~~ A talk by Wilf on generalizations of the Gray Code Problem, in particular relating such questions to the existence of hamiltonian cycles. [redacted]

[redacted] Their various generalizations are also of interest.

- (U) A talk by Ron Graham on quasi-randomness as a replacement for the intractable concept of random graph.
- (U) A session of invited talks on codes and dynamical systems, featuring talks by Marcus and Ashley. These dealt with sliding-block decoders, a generalization of trellis codes.
- (U) A poster session featuring work by Weinstein (de Bruijn sequences), Bart Rice (characteristic sequences in characteristic q), and Maffioli (RPP algorithms for NP-complete problems).

P.L. 86-36

EO 1.4.(c)

Problem Session

(U) At the Problem Session held Tuesday night and chaired by Peter Winkler, twenty open problems from academia were presented on which they would like to solicit research. Later, a handout was distributed giving the problems that were raised at the session. Only a single problem was answered cold at the session - and that by Andy Odlyzko (The guy is smart!) The following is a brief summary of the problems with their sources at the conference (which may not be their true originators):

- 1) (Grinstead) What is $\lim_{n \rightarrow \infty} \Pr(\text{random partition of } 2n \text{ is graphical})$?
- 2) (Voigt) Given the lattice of subspaces of an n -dimensional vector space over $GF(q)$, can the levels k through l be covered with few intervals?

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

- 3) (Richey) Can the edges of planar graph be partitioned into two pieces each of which is outer planar? series-parallel?
- 4) (Duffus) Let H be a hyperplane of $L_n(q)$, P a point not in H . Can the spaces not comparable to either be partitioned into $qn-1-1$ copies of $L_{n-2}(q)$?
- 5) (Kleitman) Let $\sum x_i^2 \leq 1$; prove that at least half of the sums $\sum \varepsilon_i x_i$, where $\varepsilon_i = \pm 1$, have magnitude ≤ 1 .
- 6) (Kleitman) Let $2n$ candies be placed on the vertices of an n -cube. You may pick up two candies from a vertex, eat one, and put the other down on an adjacent vertex. Prove that you can always get a candy to the origin.
- 7) (Tovey) Given a real square matrix, how many of its entries need to be examined to find a saddle point?
- 8) (Wilf) Fix n and let $f(j)$ be the number of ways of expressing the identity permutation on n letters as the product of j transpositions. Find out anything about $f(j)$.
- 9) (Tzvieli) (solved by A. Odlyzko) Let x_1, \dots, x_n be consecutive integers none of which is prime, for which a k exists satisfying $\gcd(x_i, k) > 1$ and $\gcd(x_i, k-1) > 1$, for all $1 \leq i \leq n$. Find $\max n$ or show n can be arbitrarily large. (AO shows the latter!).
- 10) (Kezdy) Fix d and let G be the $(2d-2)$ -regular graph on \mathbb{Z}/n , $n > 2d-1$, given by $x \sim y$ iff $|x-y| < d$ or $|y-x| < d$. Find the smallest induced subgraph H such that $\delta(H) \geq d$.
- 11) (Ullman) Consider the disjunctive product $G \times H$ of two graphs. Then $\chi(G \times H) \leq \chi(G)\chi(H)$ is known. Define $\chi(G|F) = \chi(G \times F)/\chi(F)$. Conjecture: $\chi(G \times H|F) \leq \chi(G|F)\chi(H|F)$.
- 12) (McCanna) Information is inserted into a vertex of an n -cube at time $t = 0$. At time $t=2$ it spreads to all neighbors of the vertex, and can be inserted again at a second vertex. Let $f(n)$ be the minimum time to inform all vertices. Prove $f(n) =$ the greatest integer at most equal to $(n+3)/2$, so that you can do no better than insert at P , then at the antipode of P , then wait!
- 13) (Hurlbert) What is the largest (should this be *smallest*?) $l \leq k$ for which the levels l and $2k+1-l$ of an $(2k+1)$ -cube induce a Hamiltonian subgraph? (it is well-known that levels k and $k+1$ work)
- 14) (George) Let $A = (a_{ij})$ be the adjacency matrix of an arbitrary n -regular graph. Can you replace the 1 in position ij with a number b_{ij} between 1 and n such that (1) $b_{ij} \neq b_{ik}$ for $j \neq k$, and (2) $|b_{ij} - b_{ji}| \equiv 1 \pmod{n}$ whenever $a_{ij} = 1$?
- 15) (D. West - from Maurer, Wagstaff, Slater) For what n is there a Gray code on the n -cube such that the coordinates changed at successive steps are always adjacent? (This is the well-known lamplighter problem that I wrote up in my trip report for the Boca Raton conference many years ago. I got Ralph J. interested in it then. Not much progress has been achieved.) This is believed true for small n , but false for $n = 8$. Any more information?
- 16) (Tovey) What is the complexity of finding, in a weighted complete graph a Hamiltonian circuit whose weight cannot be lowered by a two-edge exchange? (i. e. a TSP tour that is 2-optimal exists, but can we find it in polynomial time?)
- 17) (Tovey) Call the binomial coefficient $C(m, k)$ proper if $1 < k \leq m/2$. What is the greatest n such that there exists a number with n proper binomial representations? Can there be infinitely many such? (e. g. $C(16, 2) = C(10, 3)$. Erdős claims to have a number with 8 or 9 such representations!)
- 18) (Trotter) Let P be the poset of vertices, edges, and faces of a 3-dimensional polytope. It can be shown that $\dim(P) \leq 6$; what is the correct upper bound?
- 19) (Spencer) Let $A = \{S_1, S_2, \dots\}$ be a family of k -sets such that the degree of each ground element is D . Let $\chi(A)$ be the least m such that A is the union of m disjoint subfamilies P_i , and let $\phi(A)$ be the greatest m such that A is the union of m subfamilies C_i each of which is a covering subfamily. Then $\phi(A) \leq D \leq \chi(A)d$, and it is known that $\chi(A) = D(1+o(1))$ implies $\phi(A) = D(1+o(1))$. Can this implication be reversed?
- (20) (Grinstead) The average number of Hamiltonian paths in an n -tournament is $n!/2^{n-1}$. Conjecture: for n odd, all regular n -tournaments beat the average!

~~CONFIDENTIAL~~

ReviewBOOKS ON THE HISTORY of
SIGNALS INTELLIGENCEReviewed by: A28

P.L. 86-36

There are a few books on the history of signals intelligence of particular significance that I recommend to friends who ask about them.

By far, the best book I have ever read on the use of signals intelligence in war is Ralph Bennett's *Ultra in the West: The Normandy Campaign 1944-45*. Bennett worked at Bletchley Park¹ from February 1941 to the end of the war as a reporter in Hut 3. What makes the book particularly useful is that Bennett, a Cambridge don who specialized in medieval history, wrote it not only from memory of his activities during the war but also from decrypts of German ENIGMA made available to the public for the first time at London's Public Record Office in 1977.

Bennett actually wrote many of the terse reports sent to the field commanders himself and was able to reconstruct day-by-day, hour by-hour, the availability of sigint to the invasion of Normandy and the subsequent battles in western Europe. When Bennett describes a particular event or situation, he

refers to the sigint by the time a specific piece of information was passed to the commands in the field, German and Allied. That is, each ULTRA-based statement in the book is supported by one or more signals, the time of transmission by a German command, and the time of transmission from Bletchley. It is a phenomenal piece of research!

Another most significant book is R.V. Jones' *The Wizard War: British Scientific Intelligence 1939-1945*. Jones was a Scientific Officer on the staff of the Air Ministry in London during World War II and, as such, had access to the highest compartments⁴ of sigint as well as photo and human intelligence. He is held by many to be the father of scientific and technical intelligence. As the scientific adviser to MI-6 and Churchill, Jones played a crucial role in the scientific and technological struggle involving radar, navigational beams, electronic warfare and German V weapons. Jones had a unique grasp of the intelligence process -- he used elint, comint, aerial photography, prisoner interrogation and captured material. His book is a clear argument for small organizations with the close participation of its chief in analysis.

Arguably the most important book on sigint written by an American is David Kahn's *The Codebreakers: The Story of Secret Writing*. Kahn did not participate, as Bennett and Jones, in signal intelligence activities but he wrote the most lucid and most comprehensive book on cryptology up to World War II. Unfortunately, Kahn wrote his book a decade before the ULTRA secret was revealed so one has to go elsewhere for sigint history concerning the European theater in WWII. But Kahn does chronicle a complete history of cryptography including ancient secret writing, the Black Chambers, the interest by Thomas Jefferson, World War I, Yardley, Friedman, NSA, etc.

Another important book on sigint written by an American and largely unnoticed is *The ULTRA Americans: The U.S. Role in Breaking the Nazi Codes* by Thomas Parrish. As Parrish relied heavily on records and interviews with "ULTRA Americans", he tells the fascinating story of ULTRA as seen from an American viewpoint. The book offers some insights into the use and handling of this most precious source of intelligence by operational commanders, including notably Patton and his Third Army, but its most significant revelation is the work

EXPLANATORY NOTES

Bletchley Park was the home of the British Government Code & Cipher School (GC&CS), forerunner of GCHQ.

Hut 3 was the area for translation of the decrypts and reporting of German Army and Air Force activities. Hut 6 was the area for decryption. Huts 8 and 4 were the equivalent areas for the exploitation of German naval communications.

ENIGMA was the name of an cipher machine patented in 1919 and originally marketed as a means to safeguard commercial secrets in Germany. It was eventually used by all branches of the Wehrmacht.

ULTRA was the highest level comint compartment at the time; it was the category for the results of UK-US exploitation of German high-grade cipher.

of the joint U.S.-British mission, undertaken after the war was won to determine the success of the German signals intelligence service and its subsequent discovery of the German achievement against Russian high-level enciphered teleprinter communications. There is little doubt that the Americans owed much to the British regarding the exploitation of the German ENIGMA transmission during the war just as the British were in debt to the Poles for their techniques passed on to them immediately prior to the outbreak of war in 1939. But Americans were very much part of the team at Bletchley park from late 1942, and their remembrances, sometimes folksy and always anecdotal, add greatly to our understanding of operations in the Huts at Bletchley.

Of naval operations, two books stand out. One is by Edwin Layton, *And I Was There, Pearl Harbor and Midway*. Layton was the head of intelligence for the Pacific Fleet prior to World War II and served under in that capacity for Nimitz throughout the war. Layton's memoirs provides the most definitive answer on why we were surprised in December 1941. The book is a serious, well documented history of the American intelligence effort against Japan between the wars and through the end of WWII. It concentrates mostly on the events which led up to Pearl Harbor and the decisive

naval battle near Midway Island in June 1942. For the former, Layton points out that although we had cryptanalytical success against Japanese codes, we were organizationally confused and did not take benefit of our advantage. Regarding the latter, Midway was a smashing success for our Navy and sigint played the crucial role.

The other important book on naval operations and sigint is the late Patrick Beesly's *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Center 1939-1945*. Beesly served in the OIC, the British Admiralty's organization which collated, evaluated, and disseminated all intelligence on enemy navies. He places the role of comint and ULTRA in proper perspective as an aid in winning the naval war, particularly against German submarines. The book also documents development of fusion centers on both sides of the Atlantic in support of operational naval forces.

By far the best unclassified reference book on sigint or intelligence is the several volumes by F.H. Hinsley, et al, *British Intelligence in the Second World War*. It is part of the official British history of World War II and is the most significant account of the role intelligence (in particular, sigint) played in strategy and operations in WWII. Hinsley and his colleagues, given full range to British government documents and intelligence records, revealed, for example, that the British had two sigint stations in the Soviet Union during the early days of the war and that they helped the Soviet's traffic analysts with knowledge of analytic techniques developed at Bletchley. For a serious scholar of intelligence in WWII, this book is *the* reference. (Unfortunately, there is no parallel in official U.S. history.) The history does include quite a bit on sigint relationships prior to and during World War II between the UK and the US.

Here is a list of my favorites:

ANDREW, Christopher, *Secret Service: The Making of the British Intelligence Community* (London: Heinemann, 1985)

BATES, David Homer, *Lincoln in the Telegraph Office: Recollections of the U.S. Military Telegraph Corps During the Civil War* (New York, London: D. Appleton-Century, 1939)

BEESLY, Patrick, *British Naval Intelligence 1914-1918* (New York: Harcourt Brace Javanovich, 1982)

_____, *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Center 1939-1945* (Garden City, NY: Doubleday, 1978)

BENNETT, Ralph, *ULTRA in the West: The Normandy Campaign 1944-5* (New York: Scribners, 1980)

BERTRAND, Gustave, *ENIGMA 1939-1945* (Paris: Librairie Plon, 1973)

BLAIR, Clay, Jr., *Silent Victory: The US Submarine War Against Japan* (Philadelphia: J.B. Lippincott, 1975)

CALVOCORESSI, Peter, *TOP SECRET ULTRA* (New York: Pantheon Books, 1980)

CLARK, Ronald William, *The Man Who Broke Purple: The Life of the World's Greatest Cryptologist, Col. William F. Friedman* (Boston & Toronto: Little, Brown, 1977)

CLAYTON, Aileen, *The Enemy is Listening* (London: Hutchinson, 1980)

EWING, A. W., *The Man of Room 40: The Life of Sir Alfred Ewing* (London: Hutchinson, 1939)

GARLINSKI, Jozef, *Intercept: The ENIGMA War* (London: J.M. Dent and Sons, 1980)

GYLDEN, Yves, *The Contribution of the Cryptanalytic Bureaus in the World War* (Washington, D.C.: Government Printing Office, 1935)

HINSLEY, F.H., et al, *British Intelligence in the Second World War: Its Influence on Strategy and Operations* (London: HMSO, 1979)

JONES, R.V., *The Wizard War: British Scientific Intelligence 1939-1945* (New York: Coward, McCann and Geoghegan, 1978)

KAHN, David, *The Codebreakers: The Story of Secret Writing* (London: Weidenfeld and Nicolson, 1967)

LAYTON, Edwin T, et al, *And I Was There: Pearl Harbor and Midway -- Breaking the Secrets* (New York: William Morrow, 1985)

LEWIN, Ronald Lewin, *The Other ULTRA* (London: Hutchinson, 1982)

_____, *ULTRA Goes to War: The First Account of World War II's Greatest Secret Based on Official Documents* (New York: McGraw-Hill, 1978)

MONTAGU, Ewen, *Beyond Top Secret ULTRA* (New York: Coward, McCann and Geoghegan, 1978)

MURRAY, Williamson, *Luftwaffe* (Baltimore: The Nautical & Aviation Publishing Co., 1983)

PARRISH, Thomas D., *The ULTRA Americans* (New York: Stein and Day, 1986)

SHULMAN, David *An Annotated Bibliography of Cryptography* (New York: Garland, 1976)

TUCHMAN, Barbara W., *The Zimmerman Telegram* (New York: Viking, 1958)

WELCHMAN, Gordon, *The Hut Six Story* (New York: McGraw-Hill, 1982)

WINTERBOTHAM, Francis W, *The ULTRA Secret* (London: Weidenfeld and Nicolson, 1974)

YARDLEY, Herbert O., *The American Black Chamber* (London: Faber and Faber, 1931)

Solution to :

NSA-CROSTIC #67 (plus)
4th Issue 1988

[Brigadier John H.] Tiltman, COLLECTED
ARTICLES

_____ one of my leading book breakers, worked chiefly _____ [and seemed to bully any of my attached officers who worked under her.] She is famous for her editions of Mozart's and Beethoven's letters and was reputed on one occasion to have said [to _____] "You don't seem to realize, Commander _____ that my work starts when I leave your office!"

The unadvertized feature is that the contents of cell 274 is an exclamation point!

EO 1.4. (d)



P.L. 86-36

To the Editor:

(U) [redacted] in his article entitled "Changes In Agency Reporting" (CRYPTOLOG, 3rd Issue 1988), presented an excellent perspective on the most recent changes in Agency reporting philosophy. In his last paragraph, "Where Are We Headed" he mentions some of the problems facing Agency reporters in the future. In addition to his observations I would like to offer some of my own which I think will have a major effect on the future of SIGINT reporting here at NSA.

~~CONFIDENTIAL~~

[redacted]

(U) Is the Training School presently capable of providing this type of training? If not, it will take some time to devise courses, and provide the training required for an adequate number of reporters. We probably need to start soon

[redacted] is upon us. As we have found out in the world of collection, technology quickly outpaces whatever we have in our arsenal. The same will be true for SIGINT reporting unless we take the first steps soon.

~~(FOUO)~~ Fortunately some of the technology that is the problem is also part of the solution. By using graphics software, scanning technology, desktop publishing, etc., our reporters can begin to keep pace with our customers' requirements for information. We will probably have to take a hard look at the way we are producing and disseminating reports. The old "E-GRAM" will have to take on a new look to incorporate both text and graphics in the same document. If we don't take steps soon we won't be able to meet our customers' demands for information. If we don't begin to make some changes in our reporting philosophy and procedures we could be in danger of merely collecting the customers' required information and passing it on to him, as collected, for him to make an evaluation of the content. We could end up being nothing more than a transmitter of SIGINT information to our consumers rather than reporters of SIGINT information.

[redacted] Chief, G82

P.L. 86-36

→
To the Editor:

~~(FOUO)~~ T is not the only Key Component with a "Yellow Pages." The Information Systems Security Organization has just completed an INFOSEC Yellow Pages and a Services Directory. A hard copy of our Yellow Pages will be out within the next couple of weeks and an automated capability is expected by the summer. The automated system will have several search capabilities to aid users within the INFOSEC organization.

(U) Our Yellow Pages were the result of an employee suggestion at a "Town Meeting" held by our former DDI. Your editorial [3rd Issue

1988] and [redacted] response [4th Issue 1988] would seem to indicate that "Look it up in the Yellow Pages" can be an appropriate response in some organizations.

[redacted] D/Chief, S1

←
To the Editor:

(U) In response to [redacted] article in the 4th Issue 1988 of CRYPTOLOG entitled "The Question of Leadership," I am happy to report that in the 30 to 40 years since [redacted] was at sea, many changes have occurred.

(U) Today's Navy is an all-volunteer force made up of officers and enlisted personnel with significantly broader and more extensive education and training than [redacted] experienced in the 1950's. The World War II ships of that time have been replaced by modern and highly complex warships which require a very high degree of technical competence and management (leadership) ability to operate.

(U) One fact that [redacted] noted is still true. That is that the appearance, morale, and operational performance of a ship is a reflection of the competence, ability, and personality of its commanding officer. This fact, coupled with the self-contained, self-sufficient and independent "on-their-own" nature of a ship at sea, results in a unique relationship and dependency between captain, officers, and crew that is not duplicated elsewhere. Unless you have experienced sea duty you might not realize that once a ship has sailed (steamed) over the horizon it is out of the country. In fact, it isn't in any country! At that time the realization of the captain's role and the relationship between him and the crew is much easier to see. Among other things, the captain is the senior leader, the standard setter and the one individual above all others on board, who is responsible for the ship and all hands aboard.

(U) It is quite obvious that those experiences at sea back in the 50's made a lasting impression on [redacted] and partially influenced his own leadership (management) abilities.

(U) Go Navy!

P.L. 86-36

R. A. Schriver, Capt., USN, Asst Commander,
Naval Security Group Command

~~SECRET~~

CLASSIFICATION QUIZ



JAMES C. LEISTER, DDO/CAO

~~(S-CCO)~~ This multiple-choice quiz illustrates some of the common classification decisions many of us must make on a regular basis.

1. Sensitive Compartmented Information (SCI) refers to which of the following:

- a. TK
- b. COMINT
- c. BYEMAN
- d. VRK
- e. Any or all of these.

2. COMINT which, if compromised, would allow the target country to take specific countermeasures to deny us further access, must be handled as:

- a. TS
- b. S-CCO
- c. TK
- d. COMINT codeword.

3. The "fact of " a COMINT relationship between NSA and GCHQ, CSE, GCSB, or DSD is:

- a. S-CCO
- b. CONFIDENTIAL
- c. TS
- d. FOUO.

4. The fact that there are categories of COMINT, e.g., "cleared for CAT III COMINT," must be:

- a. C-CCO
- b. FOUO
- c. SECRET
- d. UNCLASSIFIED.

5. A SIGAD, e.g., USA-57, when associated with its location (Clark AFB) or its

administrative designator (6922 ESS), must be classified at least:

- a. SECRET
- b. C-CCO
- c. CONFIDENTIAL
- d. FOUO.

6. The fact of the existence of Third Parties, without elaboration, must be protected as:

- a. CONFIDENTIAL
- b. FOUO
- c. C-CCO
- d. UNCLASSIFIED
- e. S-CCO.

7. The "Handle via . . ." channels caveats for COMINT, BYEMAN, TK, and/or LOMA must be handled as:

- a. FOUO
- b. C-CCO
- c. SECRET
- d. CONFIDENTIAL.

8. All GAMMA information must be classified at least:

- a. S-CCO
- b. SC
- c. CONFIDENTIAL
- d. TSC.

9. The statement "cleared for TOP SECRET, Special Intelligence (cleared TS/SI)" is:

- a. FOUO
- b. CONFIDENTIAL
- c. UNCLASSIFIED

~~SECRET~~~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

10. The "fact of" NSA's SIGINT support to NATO and NATO Commands is:

- a. CONFIDENTIAL
- b. SECRET
- c. FOUO
- d. S-CCO.

11. Which of the following should not be marked on SAO (candy-stripe) coversheets:

- a. COMINT codewords
- b. BYE projects
- c. NOFORN
- d. VRK-11A
- e. TK codewords.

12. NSA's association with SUSLOL, SUSLOO, SUSLOM, is:

- a. CONFIDENTIAL
- b. FOUO
- c. UNCLASSIFIED
- d. C-CCO.

P.L. 86-36

13. Another marking that should always accompany LACONIC is:

- a. ORCON
- b. PROPIN
- c. NOCONTRACT
- d. NOFORN
- e. None of these.

(Answers on page 18)

minicrypts #2



by Bill Lutwiniak, P1

Editor's note: We had only one response to the minicrypts in 4th Issue 1989. Astonishing for this Agency! But a reader pointed out that the fact that Bill Lutwiniak composed it would intimidate people; it sure gave him cause to pause, and he's still pausing!

Let's try one more time. Bill tells us that this one is not so hard. Do let us know whether you like it or not, or even, whether you'd even bother to try it.

Solution to

MINICRYPTS, 4th Issue 1988

- 1. WALRUS PUPS SPRAWL
- 2. HEDGEHOGS DO SO SHED
- 3. LITTLE GIRL BETTER LET BIG BEE BE

The Winning (and only) entry came from the team of:

and "Mother" [the MASS4 computer].
The team won a CRYPTOLOG mug, and promised faithfully that all members would share it equally.

~~FOUO~~

1. WUBGLSITHING

GYFLHGT RUSHUN

WBGNFIRUYLUH

2. *TRUTH TODUSTED UR

UH SATED TOD

3. TRGA DRIVYL

DELIVYER GRETA

* denotes a proper name

~~This puzzle is FOUO~~

P.L. 86-36

~~SECRET~~~~HANDLE VIA COMINT CHANNELS ONLY~~

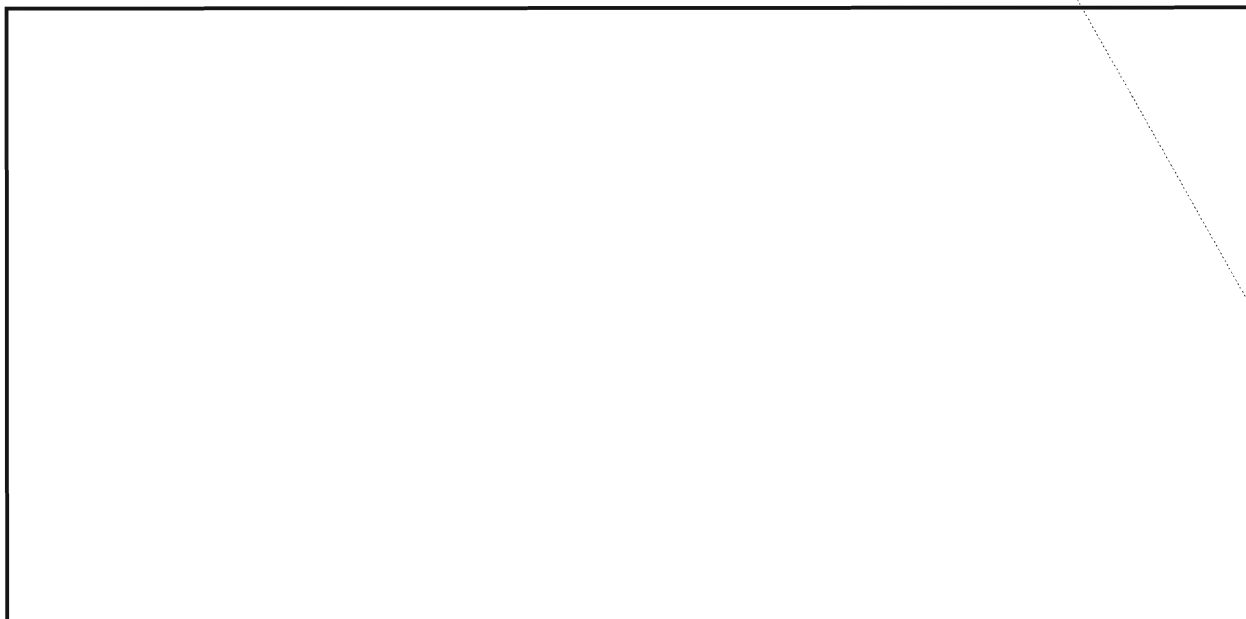
HOW TO SOLVE A DOUBLE-CROSTIC

Using the Definitions, fill in whatever Words you can. Then copy each letter from the Words into the corresponding square of the grid below. Scan the text in the grid from time to time; from the recovered fragments you may be able to complete the word in context. Copy the new entries from the grid into the Definitions, where the fragments there might suggest a complete Word, and so on, working back and forth. Also, scan down the first positions of the Words as you recover them for additional clues.

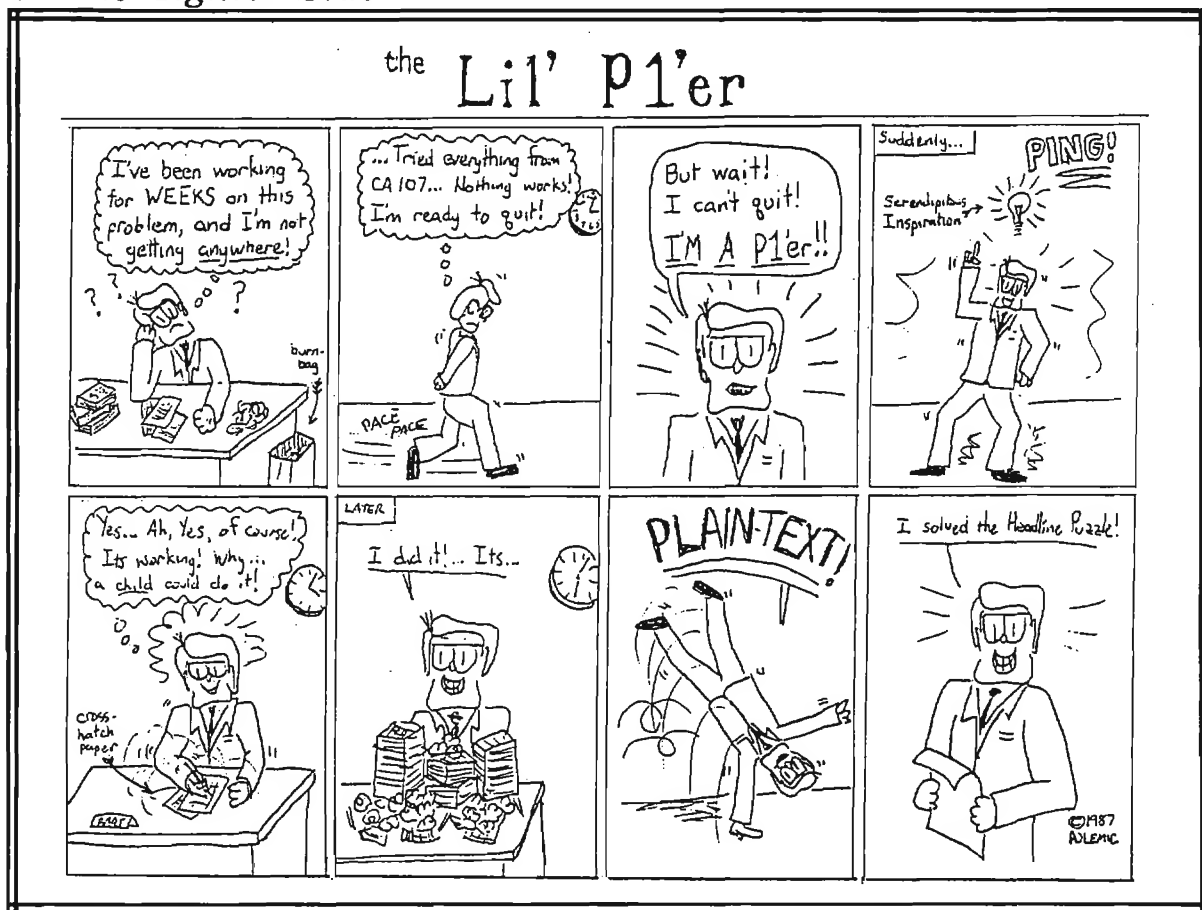
DEFINITIONS

WORDS

The quotation in the grid was taken from an article that appeared in an NSA publication. The author's name and the title of the work are spelled out in the first positions of the WORDS.

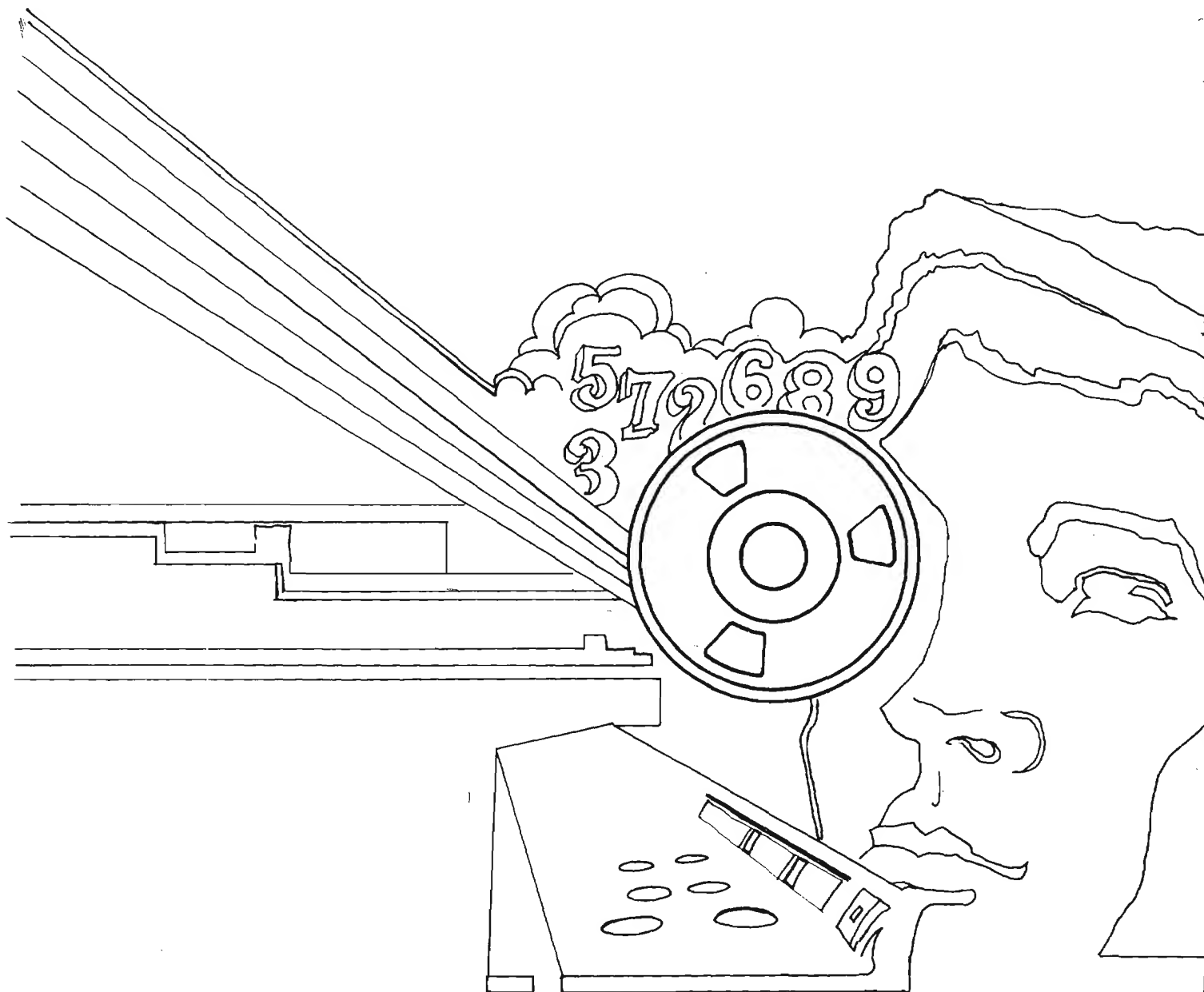


On the Lighter Side



Courtesy of Polemics

~~TOP SECRET~~



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~NOT RELEASABLE TO CONTRACTORS~~